

ContentProtect Pro

Administrator User Manual

Instructions for Installing and Using the Application

Table of Contents

Table of Contents.....	2
Welcome to ContentProtect Pro.....	4
Sources of help.....	4
System Requirements and Key Features.....	5
System Requirements.....	5
Getting Started	6
Install from the World Wide Web	6
Installation from a CD	9
Setup Wizard.....	9
Signing In as an Administrator	10
ContentProtect Pro Admin Utility Application.....	10
User Preferences	11
Organization Overview	11
Organization Profile.....	11
Set Organization Restrictions	12
Categories	13
Category Descriptions.....	13
Groups Overview	15
Group Profiles.....	15
Set Group Restrictions	15
Create New Groups.....	16
Delete a Group	16
Reassigning Users to Groups.....	17
User Overview	17
User Profiles.....	18
Status.....	18
Password	18
Options.....	18
Import a User's Account to a Specific PC	19
Set User Restrictions.....	19
Create New Users	20
Delete a User.....	22
Reassigning Users to Groups.....	22
URLs.....	22
Notifications.....	22
Administrators Overview.....	24
Adding a New Administrator.....	24
Deleting an Administrator.....	24
Editing Administrator Privileges	25
Reporting Overview	25
Access Reports.....	25
Report Coverage	25
Date Range.....	25
Customizing Report Defaults.....	26

Chat (IM) Reports	26
Time Spent in Chat	26
Chat Messages	27
Chat Apps.....	27
Chat Sites	27
Chat Report Detail	27
Web Reports.....	28
Time Spent Online	28
Web Usage	28
Categories Logged	28
Filter Actions	28
Web Report Detail	29
Recategorizing from Second Level Reports	29
Glossary	30
Frequently Asked Questions	32

Welcome to ContentProtect Pro

Congratulations! You now have the most comprehensive—and yet most easily adaptable Internet filtering software available today. However, we realize that not all organizations have the same needs, which is why we have developed **ContentProtect Pro's** unique filtering process, which is customizable for your organization.

Sources of help

The following is a list of help sources for **ContentProtect Pro**.

1. The **ContentProtect Pro** User Guide (PDF format) – Available on-line to Administrators
2. Step-by-step instruction (Quick Start Guide)
3. **ContentProtect Pro** category list with descriptions – Only available to Administrators online by clicking the category link and also listed below.
4. FAQs (Frequently Asked Questions)
5. **ContentProtect Pro** Web-based reporting
6. Prompt, competent, and courteous **Customer Support** by calling **1-800-485-4008** for questions and technical assistance. Customer Support is available Monday through Friday, 8 a.m. to 5 p.m. Mountain Standard Time.
7. You can email your questions any time to info@contentwatch.com.

System Requirements and Key Features

The following list explains the system requirements for **ContentProtect Pro** and the key features.

System Requirements

- PC with Pentium or compatible 133 MHz or faster processor
- Microsoft Windows 98SE/Me/2000/XP
- 64 MB RAM
- 100 MB hard drive space
- Color monitor with a minimum 800x600 resolution
- Internet connection
- Internet Explorer 5.0 or greater, Netscape 6.0 or greater

Key Features

- Online organization management
- Online group management
- Online user management
- User-friendly interface
- Client-based filtering
- Server-based category settings
- Unique and portable user profiles
- Web-based drill-down reports
- Blocked site override option
- Email notifications of inappropriate Internet usage
- Online activity reports on Chat (IM) and Internet activity
- Online URL recategorization

Getting Started

To begin using **ContentProtect Pro**, follow the instructions below:

1. **Set up your organization's account** and create an administrator user account.
2. **Install the Client on each computer** (this step can be accomplished by the system administrator or the user). During the install, if the user account does not already exist, it will be created.

Note: After installation and upon logging into **ContentProtect Pro** (if login is required), each workstation will assume the default Internet settings. Specific user account settings can be set in the online management application by an organization or group administrator.

3. **Log in to the online management application** (<https://ce.contentwatch.com/>). When prompted, enter your organization account name, administrator username, and password.

With this application you can:

- Add and modify user and group profiles (including Internet settings)
- Assign users to groups
- Re-categorize URLs
- Add Notification Rules to notify you of possible inappropriate activity

You can set up specific Internet settings for:

- Giving other users administrator privileges
- Viewing Internet activity reports from within your organization for the entire organization or by user or group.

Install from the World Wide Web

To install **ContentProtect Pro** from the World Wide Web, follow the instructions below:

1. Access the following Web site:

<https://cemaster.contentwatch.com/CEMaster/>

2. Before installing **ContentProtect Pro** on each computer, you will need to create your organization's account. When you purchased the product you received a 16-digit registration number and a link to the online setup. (If the account was set up for you or you already have an account, skip to "Account Setup and Installation"). The registration number only needs to be entered once to begin the setup process and may not be used again.
3. Enter the 16-digit registration number you received from ContentWatch in an email prior to creating your organization.
4. Enter the appropriate organization information in the respective fields (All fields are required.):

Enter the name of your organization:

This will be used for display purposes in the reporting and online management application.

Create an account name:

This will be needed during the installation of the client application and is designed to identify members within a given organization.

(4-20 alpha-numeric characters)

Create an install password:

This will be used to install **ContentProtect Pro** on individual user machines.

(4-20 alpha-numeric characters)

Create an uninstall password:

This will be needed to uninstall the client application from personal computers. This should be kept confidential and be different from the install password.

Anyone with the uninstall password can remove

ContentProtect Pro from their computer.

(4-20 characters, no dashes or spaces)

5. Click **Next**.
6. Enter the appropriate Organization Administrator information in the respective fields:

First and last name:

This is used to identify you in the Online Management application and reports.

Email address:

Enter the address that you would like notifications of inappropriate Internet activity to be sent to. This address will also be used to send you a confirmation email when the setup process is complete.

Create an Administrator user name and password:

You will need the Administrator user name and password to sign in to the Online Management application, which you would go to in order to add and modify users' profiles, create other Administrators and view reports.

(4-20 alpha-numeric characters)

7. Click **Next**.
8. Verify the information you just entered is correct and print a copy of it for your records, click **Next**.
9. A *What's Next?* screen will display with the following message:

Congratulations! You've successfully set up your Organization's Account. You can now install the application on personal computers that will be monitored and filtered. An

email has been sent to you with a download link and instructions on how to install the client software. The e-mail also contains the Organization Account Name and Install Password, which will be needed. To save time, forward this email to anyone that needs to install this application on his or her computer.

To download the application now, click on the link below:
<http://cemaster.contentwatch.com/CEMaster/download.html>

10. Access the following Web site to download the software to your computer:

<http://cemaster.contentwatch.com/CEMaster/download.html>

Click **Download Now**.

11. A download window will display. Select **Save**. Designate where you want to save the file on your computer. Click **OK**.
12. Double-click the downloaded file (wwesetup.exe) on your hard drive and follow the on-screen directions to begin the installation.

Installation from a CD

Note: You must have an Internet connection to install **ContentProtect Pro**. If you have a dial-up connection, you should connect to the Internet and close all applications before installing.

To install the software from a CD, follow the instructions below:

1. Insert the CD into the CD ROM drive (If the CD does not automatically run, go to Start>Run type in “d:Autostart.exe” Replace the D with the letter for your CD-ROM drive.)
2. From the Menu, select Install Software; this will open the Setup Wizard.
3. Click **Next** to start the Setup Wizard.

Setup Wizard

Once the Setup Wizard displays, you are ready to install **ContentProtect Pro**.

1. Click **Next** on the Welcome screen.
2. Choose to accept the license. Click **Next**.
3. Choose the Install directory. Click **Next**.
4. Select the products to install. You must install ContentProtect Professional. Click **Next**.
5. Enter the Organization Account Name and the Install Password. Your administrator should have provided these; contact your administrator if you do not have the account name and password. Click **Next**.
6. Enter all of your user information. The Email field is not required, but it is recommended. Click **Next**.
7. Verify your settings and then click **Install** on the confirmation dialog.
8. Click **Finish** to restart the computer and complete the installation.
9. When the machine restarts, run the Online Updates. You can launch this from any of the products or by selecting it from the right-click menus of the taskbar icons located at the bottom of the screen next to the clock.
10. When the update dialog displays, click **Check For Updates**.
11. If the default settings have not been changed, the new updates will download and install automatically. If the default settings have been modified, follow the prompts to download and install updates. When the process is complete, select the “Click here to restart your computer now” link.
12. Your system should now be fully updated with the newest version of **ContentProtect Pro**.

Signing In as an Administrator

After the **ContentProtect Pro** organization has been created, you need to define the user profiles for the specific groups and/or workstations in your organization. You must first sign in to the online management application as an administrator to modify user profiles. You set up an administrator account during the organization setup, so it is simply a matter of signing in with your organization account name, administrator username and password.

ContentProtect Pro Admin Utility Application

This utility can be used on individual computers to:

1. **Find out which user is currently signed in** on the current PC
2. **Sign users in and out**
3. **Force changes made online to take effect immediately:** There is a wait period of up to an hour for changes made through the online management application to automatically take effect.
4. **Display license information** (This may be needed for customer support.)

This utility can be run from a CD, floppy, network, or hard drive. It does not need to be installed.

Note: This utility is not needed unless the Client User Interface (UI) is hidden except to view license information. If the Client UI is not hidden, you can perform all these tasks within it. We recommend not copying this utility to computers not run by administrators.

To download the utility:

1. Login to the online management application.
2. Click on the **Downloads** link next to Sign Out.
3. Click on the **Download Now** button for the **ContentProtect Pro** Admin Utility application. A dialog box will display asking you where to save the file. Once the utility is downloaded, simply run the utility by double-clicking the icon or filename of the downloaded file. You will need to log in with the administrator user name and password.

User Preferences

To setup your **ContentProtect Pro** preferences, follow the instructions below:

1. Access the following Website:

<https://ce.contentwatch.com/>

The **ContentProtect Pro** login page will display.

2. Enter the login information that you created when you setup your account. Click **Go**. Your specific organization *Management* page will display.

The following preference levels can be set from this page:

- Organization
- Group
- User
- URLs
- Notifications
- Administrators

Organization Overview

All settings made to an organization are inherited by all groups and users. Group or user settings can be made more restrictive, but not less.

From the Organization page you can:

1. **Modify the organization name** (for display purposes only. This is NOT the account name).
2. **Change the install and uninstall passwords** (These are needed to install and uninstall **ContentProtect Pro** on individual computers).
3. **Choose to log Web and Chat (IM) protocols for the entire organization** (Chat protocols include AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger).
4. **Allow access to Web, Chat (IM), Peer-to-Peer and Newsgroups protocols for the entire organization** (Peer-to-Peer applications include those using the Gnutella network. For a list of these applications visit <http://www.gnutella.com/connect/>.)
5. **Adjust filter settings in each category to Warn, Block, or Allow** (Next to a category name, select an action (Warn, Block or Allow) for that category by choosing from the drop-down bar. For more information see *Categories*).

Organization Profile

A profile is made up of names, passwords, protocol settings and filter settings (i.e. whether to warn, block, or allow Web content of specific categories).

Create the Install Password - The password needed to install the **ContentProtect Pro** application on individual computers.

Create the Uninstall Password - The password needed to uninstall the **ContentProtect Pro** application from individual computers.

Web, Chat, Peer-to-Peer, Newsgroups - To allow users access to the Web, Chat, Peer-to-Peer, and Newsgroups, check the **Access Allowed** box below the main tabs. **Note:** User access can be denied through group or user settings.

Logging Users' Activity - To log user activity, check the **Log** box below the Access Allowed box. All user activity will be recorded and displayed in the Reporting section. Only Web and Chat allow logging.

Set Organization Restrictions

1. Click the **Organizations** link. The *Settings* page will display. This screen allows you to set organization-wide filter settings, enable or disable organization protocols and change install passwords.
2. In each of the categories listed there is a drop down menu located to the right that allows you to set the following restrictions:

- ☐ Allow - allow user access to sites containing content in the category
- ☐ Warn - warn the user the site may contain objectionable material in the category
- ☐ Block - block the user from sites containing content in the category

For each of the categories set the desired restriction level for the entire organization. Group or User settings can be made more restrictive than the organization settings, but not less.

3. Click the **Apply** button to affect the changes.

Categories

The best way to determine the category of a site is to examine the contents. Once you know the information a site contains you can more easily assign it to a category. Sites in a given category usually contain the same type of links, images, and text.

Note: Some sites will be categorized with multiple categories unless the site is manually recategorized.

ContentProtect Pro does the examining for you and determines the category of a requested Web page. After the category is determined, filter settings (Allow, Warn, or Block) are then applied.

Note: An administrator of a particular group can set a category action to be more restrictive but not less restrictive than the parent group. (e.g. If the Organization action for Adult/Mature is set to *Block*, no group or user settings within that organization can be set to *Warn* or *Allow*. However, if the Organization action is set to *Warn*, an administrator can change the action for a group or user to *Block* or *Warn* but not *Allow*. If the Organization's action is set to *Allow*, any group or user's action within that organization can be changed to *Warn*, *Block*, or *Allow*.

Category Descriptions

Ads - Advertisements for products, services, etc.

Adult/Mature - Sites or resources that contain subject matter intended for mature audiences, such as obscene or vulgar language and adult Chat rooms. These sites could be considered R-rated.

Chat Site - Sites or resources that contain information on Chat protocols or applications, links to Chat organizations, rings, and rooms.

Drugs/Alcohol - Sites or resources that contain subject matter that deals with the manufacturing, distribution, or obtaining illegal drugs, alcohol, or other controlled substances. Sites that depict drug or alcohol paraphernalia and/or include methods for obtaining or manufacturing them. Does not include sites that provide information on prescription medications except those sites that describe how to illegally obtain them.

Email - Sites or resources that provide access to email services, and applications.

Employment/Career - Sites providing information on employment opportunities and resources for expanding career options.

Family Resources - Sites or resources that provide family counseling, family safety tips, parenting information and tips, and family planning.

Financial/Stocks - Sites or resources that provide information about finances, financial planning, insurance, stock tickers, stock reports, or sites that allow the sell and purchase of stock. Includes banks and credit unions, and credit rating and reporting sites.

Gambling - Sites or resources that allow a person to wager money on online games with the expectation of winning money or prizes. Sites that contain links to other gambling sites or provide information on gambling strategies or tactics.

Games - Sites or resources that provide access to online or downloadable games, or discussions about games. Sites that provide information about game cheats.

Government - Sites or resources that are specific to local, state, or federal government organizations or agencies, including political party sites and specific, official political sites. Sites ending in .gov.

Hate/Violence - Sites or resources that promote or depict violence against persons, animals, property, or nations. Sites that single out groups for violence based on race, religion, or creed.

Health/Medicine - Sites or resources that deal with or provide information on mental or physical health issues. Sites that allow the online purchase of prescription medications.

Illegal Activities - Sites or resources that provide information about the manufacture, alteration, or sales of weapons. Sites that promote or depict disorderly conduct, or that provide information on the manufacturing of explosives and explosive devices.

Instructional - Sites or resources that contain instructional material, tutorials, or how-to pages.

Intimate Apparel - Sites or resources that display models wearing underwear, lingerie, or other suggestive or see-through attire, including swimsuits.

Kids - Sites or resources intended for children, including entertainment, education, crisis counseling, and kid-friendly communities.

Music/Entertainment - Sites or resources that provide access to free downloadable or for-pay online music and video files such as MP3, WAV, MPG, and AVI, etc. Sites that sell music or videos, or that are dedicated to the music or entertainment industry. Sites that provide information on TV programs and programming, including movie review sites.

News - Sites or resources that provide live, recorded, or written reports or editorials about current events.

Personals - Sites or resources that contain personal ads, personal info pages, and personal portals.

Pornography - Sites or resources that are meant to sexually arouse the viewer. May show models or real people that are engaged in erotic behavior intended to cause sexual excitement. May describe sexually explicit activities or contain sexually explicit material including images, movies, or text. Sites would be considered X-rated.

Religious - Sites providing information on specific religions or general religious resources.

Schools/Colleges - Sites or resources that contain information dealing with colleges, schools, seminars, or courses. Sites that end with edu.

Search Engines/Portals - Sites or resources that provide mechanisms for searching the Internet by specific words or phrases and that display the results as either links or images. Sites that allow a user to customize the look or content and that are geared to providing a starting place on the Internet.

Shopping - Sites or resources that provide access to online malls, catalogs, or auctions, including classified ads. Department store sites, retail store sites, or sites that have coupons for free or discounted items.

Sports - Sites or resources for sports information including amateur, college, and professional sports.

Travel - Sites or resources that provide travel information ranging from general information to booking reservations.

Work Related - Sites or resources that provide information related to a user's work.

Groups Overview

Using multiple groups is **optional** but makes changing settings and reporting more manageable. For example, you can view reports on a group that will tell you how a specific department in an organization is using the Internet. You can also change Internet settings for all members in a particular group at the same time.

From the group page you can:

1. **Modify the group name** (for display purposes only)
2. **Choose to log Web and Chat (IM) protocols for users assigned to this group** Chat protocols include AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger. **Note:** If the group's Log checkbox is checked, a user cannot change this setting. Also, if logging is enabled on the organization it cannot be disabled on the Group or User level.
3. **Allow access to Web, Chat (IM), Peer-to-Peer and Newsgroups protocols** Peer-to-Peer applications include those using the Gnutella network. For a list of these applications visit <http://www.gnutella.com/connect/>. **Note:** If the group's **Access Allowed** checkbox is not checked for a particular protocol, no users assigned to this group will be able to access that protocol.
4. **Adjust filter settings in each category to Warn, Block, or Allow** This will affect only members assigned to this group

Note: User settings can be made more restrictive than the organization or group's but not less restrictive.

Group Profiles

A group profile is made up of names, protocol settings and filter settings (i.e. whether to Warn, Block, or Allow Web content of specific categories) that affect all members of the group.

To modify a group's profile, follow the instructions below:

1. Click on the **Groups** button in the navigation menu to view the **Group List**. The groups will display alphabetically.
2. Click on the group name to view and/or modify the profile.

Web, Chat, Peer-to-Peer, Newsgroups - To allow users of this group access to the Web, Chat, Peer-to-Peer, and Newsgroups, check the **Access Allowed** box below the main tabs.

Note: User access can be denied through group or user settings.

Logging Users' Activity - To log user activity within this group, check the **Log** box below the Access Allowed box. All user activity will be recorded and displayed in the Reporting section.

Set Group Restrictions

1. Click the **Groups** link. The *Group Lists* page will display.
2. Click on the name of the group you want to modify. This screen allows you to set group wide filter settings and enable or disable group protocols.

3. In each of the categories listed there is a drop down menu located to the right that allows you to set the following restrictions:

- ☐ Allow - allow user access to sites containing content in the category
- ☐ Warn - warn the user the site may contain objectionable material in the category
- ☐ Block - block the user from sites containing content in the category

For each of the categories set the desired restriction level for the current group. Group or User settings can be made more restrictive than the organization's but not less.

4. To set group level restrictions regarding Chat rooms, Peer- to-Peer access, and Newsgroups, click the appropriate tab at the top of the page and enable or disable access to these areas.
5. Click the **Apply** button to affect the changes.

Create New Groups

1. Click the **Groups** link. The *Group Lists* page will display.
2. Click **Add New Group**. A *Settings* page will display. This screen allows you to set group-wide filter settings and enable or disable group protocols.
3. Enter the name of the group in the **Group Name** field.
4. In each of the categories listed there is a drop down menu located to the right that allows you to set the following restrictions:

- ☐ Allow - allow user access to sites containing content in the category
- ☐ Warn - warn the user the site may contain objectionable material in the category
- ☐ Block - block the user from sites containing content in the category

For each of the categories set the desired restriction level for the current group. Group or User settings can be made more restrictive than the organization's but not less.

5. To set group level restrictions regarding Chat rooms, Peer- to- Peer access, and Newsgroups, click the appropriate tab at the top of the page and enable or disable access to these areas.
6. Click the **Apply** button to affect the changes.
7. To add additional groups, click the **Groups** link and repeat steps 1 through 6.

Delete a Group

1. Click the **Groups** link. The *Group Lists* page will display
2. Click the **Delete** link located to the right of the group. A *Confirmation* screen will display
3. Click **OK** to confirm the deletion. (Note: The default group cannot be deleted.)

Reassigning Users to Groups

1. Click the **Users** link. The *Users List* page will display.
2. Check the box to the left of the users names you want to reassign.
3. Select the group you want to assign the users to from the Move selected users to group drop down menu.
4. Click the **Submit** button.

User Overview

User profiles contain settings and information for a specific user. From the users pages you can:

1. **Add and delete users**
2. **Modify user information** (name, email address and password)
3. **Assign user to a specific group**
4. **Disable Internet use** (Internet, Chat (IM), Peer-to-Peer, and Newsgroups)
5. **Allow user to override blocked messages**
6. **Enable automatic login**
7. **Show or hide ContentProtect Pro interface on user's personal computer**
8. **Allow user to request blocked pages to be re-categorized**
9. **Choose to log Web and Chat (IM) protocols** (Chat protocols include AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger)
10. **Allow access to Web, Chat (IM), Peer-to-Peer and Newsgroups protocols** (Peer-to-Peer applications include those using the Gnutella network. For a list of these applications visit <http://www.gnutella.com/connect/>)
11. **Adjust filter settings in each category to Warn, Block, or Allow.**

Note: User settings can be made more restrictive than the organization or group but not less restrictive.

User Profiles

To modify a user's profile:

1. Click on the **Users** button in the navigation menu to view the **User List**. Users are listed alphabetically, under the assigned group's heading
2. Click on the user's name to view and/or modify his/her profile.

Status

If **Yes** is checked under **Disable Internet Use**, the user's account will be disabled.

Password

This password is used to:

1. Login to **ContentProtect Pro**
2. Override blocked Web pages (if option is allowed)
3. Log in to the reports and system management (administrators only).

Options

- **Override blocked message:** If **Yes** is checked, the user is able to override any Web page that is blocked by using his or her password. Overridden Web pages are reported if logging is enabled.
- **Auto client login:** If **Yes** is checked, users will be automatically logged in to use the Internet
- **Show client user interface:** If **Yes** is checked, users will be allowed to view their profile and settings on their personal computer. The user will also be able to refresh their profile manually to force changes to take effect immediately.
- **Show Request Recategorize button:** If **Yes** is checked, users will be given the option to request that a blocked site be recategorized by an admin. For more info on Recategorization, click [here](#). (Note: If the client user interface is visible, the user may request URL recategorizations from within it, even if this option is not set to Yes.)

Web, Chat, Peer-to-Peer, Newsgroups - To allow users access to the Web, Chat, Peer-to-Peer, and Newsgroups, check the **Access Allowed** box below the main tabs. **Note:** User access can be denied through organization, group or user settings.

Logging Users' Activity - To log user activity, check the **Log** box below the Access Allowed box. All user activity will be logged and displayed in the Reporting section. Logging is only available for Web and Chat access types.

Import a User's Account to a Specific PC

If a user's account has already been created in the online management application, or by installing **ContentProtect Pro** on another computer, the same settings can be imported to another computer.

1. Begin the **ContentProtect Pro** installation and type in the user name and password you would like to import. The account information and settings will automatically be imported to that computer.

Note: It is not necessary to import a user account if the client software has already been installed. A user that has been previously created by either installing on another computer or by the administrator in the online management application, can simply sign in with his or her username and password. When this is done all of the user's settings are imported. User profiles are fully portable. Once the user profile exists in the online management application the user can sign in on any computer that has the client software installed.

Set User Restrictions

1. Click the **Users** link. The *Users List* page will display.
2. Click on the name of the user you want to modify. The users *Profile* page will display. This screen allows you to modify user information, adjust individual filter settings, enable or disable protocols for an individual, change passwords, and enable override options.
3. In each of the categories listed there is a drop down menu located to the right that allows you to set the following restrictions:
 - ☐ Allow - allow user access to sites containing content in the category
 - ☐ Warn - warn the user the site may contain objectionable material in the category
 - ☐ Block - block the user from sites containing content in the category

For each of the categories set the desired restriction level for the current user. User settings can be made more restrictive than the organization and the group, but not less restrictive.

4. The following restrictions and changes can also be set from this screen:

- ☐ Restrict user from the Internet
- ☐ Change user's Password
- ☐ Set user options

Set the desired options for each of the user settings.

5. To set user level restrictions regarding Chat rooms, Peer-to-Peer access, and Newsgroups, click the appropriate tab at the top of the page and enable or disable access to these areas.
6. Click the **Apply** button to affect the changes.

Create New Users

There are two methods that you can use to create new users.

- The first method (preferred) is through the client installation process. The way this method works is when the user installs the client software on his or her computer the information he or she enters will be compared to the users already in the system. If the account information does not match an account already in the system, the new user will be created. This method does not require any intervention by the administrator. All users created using this method will be placed in the default group as specified by the administrator on the Groups page of the online management application. The administrator can make adjustments to the user profile and/or move it into a different group as needed after the user has completed the client installation.
- The second method requires the administrator to do all of the work that is done automatically by the client installation.

To create a new user in the online management application, follow the instructions below:

1. Click the **Users** link. The *Users List* page will display.
2. Click the **Add New User** link. The *Add New User Profile* page will display.
3. In the Information section add the following information:
 - ☐ Username: enter a username in this field. (The username must be unique and if it isn't you will be prompted to enter a different username.)
 - ☐ First and Last Name: enter the user's full name in this field
 - ☐ Email: enter the user's email address in this field (This is the address where notifications will be sent if the user is made an administrator.)
 - ☐ Group: select the group you want to assign this user to from the drop down menu. (If no group is selected, the user will be placed in the default group, which appears in the dropdown automatically.)
4. Enter the user's password in the **Password** field.
5. Confirm the user's password by reentering it in the **Confirm** field.

6. In each of the categories listed there is a drop down menu located to the right that allows you to set the following restrictions:

- ☐ Allow - allow user access to sites containing content in the category
- ☐ Warn - warn the user the site may contain objectionable material in the category
- ☐ Block - block the user from sites containing content in the category

For each of the categories, set the desired restriction level for the current user. You can make the user settings more restrictive than the organization and the group settings, but not less restrictive.

7. The following restrictions and changes can also be set from this screen:

- ☐ Restrict user from the Internet
- ☐ Change user's Password
- ☐ Set user options

Set the desired options for each of the user settings.

8. To set restrictions regarding Chat rooms, Peer-to-Peer access, and Newsgroups, click the appropriate tab at the top of the page and enable or disable access to these areas.
9. Click the **Apply** button to add the new user. (Note: Clicking on any of the access type tabs will also apply changes. When changes are applied to the user profile, red text will appear under the user's profile name indicating the user profile was updated.)

Delete a User

1. Click the **Users** link. The *Users List* page will display.
2. Check the box to the left of the users' name.
3. Click the **Delete Selected Users** button. A *Confirmation* screen will display.
4. Click **OK** to confirm the deletion.

Reassigning Users to Groups

1. Click the **Users** link. The *Users List* page will display.
2. Check the box to the left of the users' names you want to reassign.
3. Select the group you want to assign the users to from the Move selected users to group drop down menu.
4. Click the **Submit** button.

URLs

Just as **ContentProtect Pro** examines each Web page request for category content to determine which category a site belongs to, the administrator(s) can re-categorize any URL. This forces a specific Web site to be categorized as the administrator specifies. Associated Filter Settings (Allow, Warn, or Block) for that category are then applied.

Consider the following example:

CommunityWatch is our community resource section accessible through the ContentWatch Website. Because CommunityWatch contains many educational articles that deal with the problems caused by pornography (and which therefore, contain some adult content) a normal filter (ours included) would block this site as pornography. After going to the site and examining the content, it would be clear that it is not pornography and should be re-categorized. Let's assume you want the URL www.contentwatch.com re-categorized as Family Resources.

To recategorize a URL, follow the instructions below:

1. Click on the **Manage Recategorized URLs** link under the URLs section.
2. Click on the **Add New URL** button.
3. Type in www.contentwatch.com and select Family Resources from the drop down list.
4. Click **Recategorize**. This site will now be compared to the category FAMILY RESOURCES and access will be warned, blocked, or allowed depending on the individual's settings for that category.

Notifications

Notifications are email messages that alert administrators of an organization or group of possible inappropriate Internet usage.

To set up notification rules, follow the instructions below:

1. Click the **Notifications** link. The Notifications page for the currently logged in administrator will display.
2. Click the **Add New Notification** link.
3. Select to whom the notification will apply by clicking the radio button next to Organization (applies to all users in the organization), Group (applies to only users associated with the given group) or User (applies only to a specific user).
4. Select a condition(s) to be notified about.
5. Click the **Add** button.

Note: Each administrator can create multiple notifications. This allows the administrator to have specific conditions assigned for specific groups and/or users if desired.

Active - To deactivate a notification, follow the instructions below:

1. Deselect the box next to the notification to temporarily disable it.
2. To permanently remove the notification, click the **Delete** link in the same row, last column.

Is Blocked - If this box is checked, a notification will be sent if a covered user is blocked from a specific Web page.

Is Warned - If this box is checked, a notification will be sent if a covered user is warned about a specific Web page.

Overrides a Block - If this box is checked, a notification will be sent if a covered user overrides a blocked Web page.

Continues from a Warning - If this box is checked, a notification will be sent if a covered user continues from a warning message.

Administrator's Overview

From the online management application, administrators can:

1. **View Internet activity reports** for the entire organization, group or user (if logging is enabled)
2. **Add and modify user and group profiles** (including Internet settings)
3. **Assign users to groups**
4. **Re-categorize URLs**
5. **Add Notification Rules** to notify them of possible inappropriate Internet use
6. **Give other users administrator privileges**

Adding a New Administrator

The first organization administrator is set up during the organization's account setup.

To create additional administrators, follow the instructions below:

1. Click the **Administrators** link. The *Administrators* page will display.
2. Click the **Add New Administrator** link. The *Administrator* page will display.
3. Select the user you want to give admin rights to from **The following USER:** drop down menu.
4. Put a check in the box to the left of each of the groups you want to give the user admin rights for.
5. Click the **Submit** button.

Note: If the administrator will manage all groups, it is only necessary to click on the organization's name at the top.

Deleting an Administrator

To delete an administrator, follow the instructions below:

1. Click the **Administrators** link. The *Administrators* page will display.
2. Click the **Delete** link located to the right of the administrator. A *Confirmation* screen will display.
3. Click **OK** to confirm the deletion.

Note: You cannot delete the original administrator. Also, this will not delete the user from the system; it will only remove the administrator privileges.

Editing Administrator Privileges

To alter the administrator's privileges, follow the instructions below:

1. Click the **Administrators** link. The *Administrators* page will display.
2. Click on the administrator's name.
3. Make changes as desired.
4. Click the **Submit** button.

Reporting Overview

ContentProtect Pro provides comprehensive Web-based reporting that is remotely accessible by any administrator in an organization. The coverage of reports an administrator can view depends upon the groups he or she manages (See Administrators section). Each chart has drill-down capability for transaction detail. Selecting the *Report Coverage*, *Date Range*, *Report Selection* (Chat or Web) and *Hourly Wage* will generate charts that report transaction detail.

Note: Logging must be enabled for any reporting to occur. You can enable logging at the user, group or organization level.

Access Reports

To access the reports, follow the instructions below:

1. Login to the Online Management application as an administrator.
2. Click the **Reporting** tab on the top navigation bar.

Report Coverage

Select the organization, group or user from the dropdown list to view reports of Internet activity. (Group administrators will not be able to select coverage for the entire organization. The group administrator will only be able to select coverage for the group(s) or users for which he or she is an administrator.

Date Range

Select a date range from the dropdown list to view Internet activity during that time frame. (If there is a very large amount of data being reported the longer the time period covered, the longer it will take the page to display the data.)

Report Selection - Select the type of reports you would like to view.

Hourly Wage - Some of the graphs use this dollar amount to determine the cost of time spent online. You may adjust this number to the average hourly wage for the organization, groups or specific users.

Note: Discrepancies between the available charts are caused by some Web pages assigned in multiple categories. As a result the charts show an approximation of Web activity and cost.

Customizing Report Defaults

You can customize the default report by clicking the **Customize Defaults** link above the graphs. You can set default options for:

- Report Coverage
- Date Range
- Report Selection
- Hourly Wage
- Time zone
- Graph style

Chat (IM) Reports

Time Spent Online, *Chat Messages* and *Chat Apps* refer to Instant Messaging applications ONLY, including AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger. *Chat Sites* refer to any Web page that is categorized as having Chat content.

Time Spent in Chat

This is a column chart that represents time spent in Chat within a specified date range.

To observe the **Time Spent in Chat** report graph, follow the instructions below:

1. Resting the mouse pointer over a column marker displays a numeric value of time spent and cost required within a specified date range.
2. Click on a column to drill-down to **Chat Report Detail** (see Chat Report Detail).

Chat Messages

This is a line chart that represents the number of messages sent within a specified date or time range.

To observe the *Chat Messages* report graph, follow the instructions below:

1. Resting the mouse pointer over an intersection between the line and graph displays the number of messages sent within a specified time or date range.
2. Click a specific portion of the line chart to drill-down to **Chat Report Detail** for that time or date.

Chat Apps

This is a pie chart that represents Chat (Instant Messaging, IM) applications used.

To observe the *Chat Apps* report graph, follow the instructions below:

1. Resting your mouse pointer over each pie wedge displays how many messages were sent using that specific Chat application during a specified date range.
2. Click on a pie wedge to drill-down to **Chat Report Detail** for that chat application (see Chat Report Detail).

Chat Sites

This is a bar chart that represents visited Chat-related Websites and the number of times that Chat site was accessed.

To observe the *Chat Sites* report graph, follow the instructions below:

1. Resting your mouse pointer over each bar displays the Chat-related Website visited and the number of times that Chat site was accessed.
2. Click on a bar to drill-down to **Chat Report Detail** for that chat site (see Chat Report Detail).

Chat Report Detail

This is a table that displays an individual user summary listing *Group*, *User*, the number of messages (*Count*), *Time Spent* and the average cost to your organization for that time (*Cost*).

To observe the *Chat Report Detail*, follow the instructions below:

1. Click a column heading to sort column data in ascending or descending order.
2. Click a **user name** to drill-down another level to the actual Chat transactions.

Time - Time is listed in ascending order and represents the time that the conversation took place.

Screen Name - This column displays the screen names of both the person sending and the person receiving Chat conversation. The user's screen name appears in red text.

Chat Conversation - This column displays the actual conversation text.

Navigation is made easy by following the instructions below:

1. Click any of the page links below the table to display *Next*, *Previous*, or a specific page of report results.
2. Click the navigation link **Graphs**, located above the table or the *Reporting* tab, to refresh Chat activity and return to reporting.
3. Click **Back** from the *browser's* toolbar to return to reporting. This will not refresh Chat activity.

Web Reports

Web-based reporting on each individual user, group or organization is remotely accessible. Each chart has drill-down capability for Web Report Detail. Selecting a user, date range, and access type (Web) will generate charts that report transaction detail.

Time Spent Online

This is a column chart that represents time spent online within a specified date range.

To observe the *Time Spent Online* report graph, follow the instructions below:

1. Rest the mouse pointer over a column marker to display a numeric value of time spent and cost required within a specified date range.
2. Click a column marker to drill-down to **Detail Report** (See Web Report Detail).

Web Usage

This is a line chart that represents the number of Web requests on an hourly or daily basis.

To observe the *Web Usage* report graph, follow the instructions below:

1. Rest the mouse pointer over an intersection of the line and graph of the line chart to display a numeric value of sites visited and cost associated with the given time frame.
2. Click on a specific portion of the line chart to generate and display **Detail Report** (See Web Report Detail).

Categories Logged

This is a pie chart that represents **ContentProtect Pro** categories that have been browsed during a specified date range.

To observe the *Categories Logged* report graph, follow the instructions below:

1. Rest the mouse pointer over any portion of the pie chart to display a numeric value of Web pages visited in each category.
2. Click on a specific portion of the pie chart to generate and display **Detail Report** (See Web Report Detail).

Filter Actions

This is a bar chart that represents filter responses to Website requests showing if a specific transaction was blocked, warned, continued after warned, overridden, or logged.

To observe the *Filter Actions* report graph, follow the instructions below:

1. Rest the mouse pointer any of the bars to display a numeric value of sites visited and cost associated with each action.
2. Click on any bar in the chart to generate and display **Detail Report** for that action (See Web Report Detail).

Web Report Detail

This is a table that displays an individual user summary listing *Group*, *User*, the number of times the Web page was visited (*Count*), *Time Spent* and the average cost to your organization for that time (*Cost*).

To observe the *Web Report Detail* follow the instructions below:

1. Click a column heading to sort column data in ascending or descending order.
2. Click the **URL** to visit the site or click on the **# of visits** to see specific access times and categories for each URL.

URL - Lists the Universal Resource Locator (URL) or address of a specific Website accessed by a user. Click any URL within this column to open the specific site in a separate window for your review.

Warning: If you are accessing reports from a remote computer that does not have **ContentProtect Pro** installed, all Websites will be fully displayed. Computers that have **ContentProtect Pro** installed will not display blocked Websites unless the administrator uses the override option or allows that specific category.

User - Lists the user account that was used to access the URL. This is the last level of report transaction.

Time - Reports the date and time the Website was accessed. This is the last level of report transaction.

Filter Action - Reports the filter action that was applied. The filter action could be Allow, Warn, Warn Continue, Block Override or Block for each category. This is the last level of report transaction.

Category - Displays the category icon(s) associated with each URL. Resting your mouse pointer over a category icon will display what that category is. Click [here](#) for a list of categories and descriptions.

Navigation is made easy by following the instructions below:

1. Click any of the page links below the table to display *Next*, *Previous*, or a specific page of report results.
2. Click the navigation link **Graphs**, located above the table or the *Reporting* tab, to refresh Web activity and return to reporting.
3. Click **Back** from the *browser's* toolbar to return to reporting. This will not refresh Web activity.

Recategorizing from Second Level Reports

To recategorize from last level report, follow the instructions below:

1. Click **Recategorize** to change the assigned category of the Website (i.e. gambling.com).
2. Select a new category from the drop-down list.
3. Click **Recategorize** to apply the changes.

Note: This will not change the category of Web pages already visited. It will change the category for future visits to the Web page.

Glossary

Administrative Privileges - Assigning a user the same access as an administrator.

Administrator - The person who is responsible for setting up and maintaining a group of users. Duties of the administrator may include uninstalling **ContentProtect Pro**, setting up and managing user profiles, assigning passwords and privileges, viewing reports, etc.

Application - Software, program, or tool used on your computer, such as a word processor, a game, or an email program.

Browser - The application that lets you navigate around and view pages on the Web. Netscape and Internet Explorer are the two most common.

Category - A general term for a whole topic or information type.

Chat - Real time communication. It is typed conversation that is received almost instantly as soon as it is sent. Talking live with one or more people via the Internet. It's like a party line, except you type instead of talk.

Client-Based Filtering - Filtering that is performed from an individual computer. Filtering software and a list of categorized sites are stored on an individual computer that makes filtering more flexible for the user making decisions about acceptable content. Aside from restricting Internet access to certain Websites, many client-based filters also offer controls for other Internet services.

Default Settings - A setting that a program is pre-set to select (usually the recommended settings) if you do not specify other options.

Drill Down - To move from a summary of information to more detailed data. To drill down through a series of reports addressing more detail at each level.

Filtering - Controlling access to a Web page request by analyzing the incoming and outgoing requests and letting them pass or halting them based on settings selected within **ContentProtect Pro**.

Icon - A small picture that represents an object or program.

Instant Messaging (IM)- Instant Messaging is the ability to see if a chosen friend, co-worker, or associate is connected to the Internet and if they are, you are then able to exchange "real time" messages with them. **ContentProtect Pro** currently can block and/or log IM activity from AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger.

Internet - The Internet consists of countless networks of computers that are connected together across the world allowing millions of people to share information. Components of the Internet include: the World Wide Web, Newsgroups, Chat rooms, and e-mail.

Log - A program or system that enters a record into a log file or report file.

Peer-to-Peer - Peer-to-Peer networks exist on the Internet and allow users to have access to other users' files residing on their hard disks. **ContentProtect Pro** is capable of blocking Peer-to-Peer activity only on the Gnutella network.

Portable User Profiles - Allows a user to login on any machine that contains the filtering software and have his or her profile imported instantly.

Remote Management - The capability of accessing files, devices, and other resources not connected directly to your workstation. In the case of **ContentProtect Pro**, reviewing report results and managing user profiles can be performed from any machine with Internet access.

Screen Name - An identifier that consists of a sequence of one or more alpha or numeric characters that uniquely identifies a person.

Server-Based Categorization and Validation - A server that maintains a list of categorized URLs (Universal Resource Locator). The server is updated regularly to ensure that all users are getting the most up to date accurate information. The server does not actually deliver the requested Web page (URL) to the customer but compares the requested URL to the list.

Shortcut Menu - A popup menu that appears by right-clicking an object. When right-clicking the **ContentProtect Pro** icon from the System Tray located in the Taskbar, the shortcut menu is displayed.

System Tray - Located on the Windows Taskbar (usually at the bottom next to the clock) contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more.

Taskbar - A system bar located at the bottom of your screen. The Taskbar is home base for the Start button, system clock, system tray, etc.

Transaction detail - Activity information based on report results.

URL - Universal Resource Locator. An address on the Internet, the URL shows the specific path that locates a site or a document online. The URL for a Web page looks like this:

`http://www.domainname/folder name/filename`

User - An individual who uses a computer.

User ID - An identifier that identifies a specific user in a program.

User Profile - Program settings that are specific to an individual user.

WWW - World Wide Web - The Web is the visual component of the Internet. Created with HTML language, Web pages can include text, pictures, sound clips, video, links for downloading software, and much more. The Web is only one component of the Internet, although the terms are often (and mistakenly) interchanged.

Web-Based Reporting - Reports that have compiled Web and Chat activity for a **ContentProtect Pro** organization and are accessible from any computer with Internet access.

Frequently Asked Questions

How do I create a new user?

See [Create New Users](#).

What is recategorization?

Just as **ContentProtect Pro** examines each Web page request for category content to determine which category a site belongs to, the administrator(s) can recategorize any URL to force a specific Web site to be categorized as he/she chooses. Associated Filter Settings (Allow, Warn, or Block) for that category are then applied. For more info see [URLs](#) (Recategorization).

I made changes online to the Internet settings. Why isn't it working?

There is a wait period of up to an hour for changes made through the online management application to automatically take effect. To force changes made to take effect immediately, use the [Admin Utility application](#). Or, if the Client UI is available for individual users, click **Refresh Profile** from the menu.

Why can't I see the report graphs?

Macromedia Flash free browser plugin is required to view the graphs. If you don't have this installed, you may get it by going to: http://www.macromedia.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash

How does ContentWatch define the categories?

See [Category Descriptions](#).

Why don't I see reports on a specific user or group?

Make sure you have privileges to view reports or modify profiles for that group or user. Also verify that logging is enabled. For more information see [Administrators](#).

Why don't I see reports of all Chat activity?

ContentProtect Pro currently is capable of blocking and/or logging IM activity from AIM (AOL Instant Messenger), MSN Messenger, and Yahoo Messenger.